Redmine - Feature #19851

Sudo mode: Require password re-entry for sensitive actions (optional)

2015-05-15 11:01 - Jens Krämer

Status:	Closed	**Start date:**	
Priority:	Normal	**Due date:**	
Assignee:	Jean-Philippe Lang	**% Done:**	0%
Category:	Accounts / authentication	**Estimated time:**	0.00 hour
Target version:	3.1.0		
Resolution:	Fixed		

Description

This patch adds a so-called sudo mode as a safe-guard against damage done through hijacked sessions, be it remotely or through physical access to a computer with an existing open Redmine session. A similar feature has been implemented for example by GitHub.

Sudo mode will require the user to re-enter his password before any potentially dangerous action is carried out (see below for full list). Once the correct password was entered, the original action will be performed and sudo mode will stay active for at least 15 minutes. Every time another action requiring sudo permissions is invoked, this interval will be reset, so more administrative work can be done without further interruptions. This behaviour is similar to what Unix sudo does.

Full list of things guarded by the patch:

- editing of account data (my/account) and email addresses
- displaying the API key, reset of rss / API keys
- editing of Project memberships
- global settings, plugin settings
- user, group, role, auth source management
- project deletion

Since actions requiring this additional authentication step are declared in controllers using a simple class method, sudo mode might also easily be used by plugins to protect their own potentially destructive actions.

This feature was developed for Planio and we think it would be very nice to have that in Redmine.

Associated revisions

Revision 14333 - 2015-06-19 20:41 - Jean-Philippe Lang

Require password re-entry for sensitive actions (#19851).

Patch by Jens Krämer.

Revision 14334 - 2015-06-19 20:43 - Jean-Philippe Lang

Changed /my/show_api_key route to /my/api_key (#19851).

Revision 14335 - 2015-06-19 21:19 - Jean-Philippe Lang

Use existing label for password submission (#19851).

Revision 14336 - 2015-06-19 21:42 - Jean-Philippe Lang

Adds a configuration setting to enable sudo mode, disabled by default (#19851).

Revision 14337 - 2015-06-19 21:43 - Jean-Philippe Lang

Renamed sudo mode test.

Revision 14338 - 2015-06-19 21:51 - Jean-Philippe Lang

Don't use SudoMode.disable! to skip API requests (#19851).

Revision 14339 - 2015-06-19 21:56 - Jean-Philippe Lang

Fixed the sudo dialog when called from a dialog, eg. email addresses (#19851).

Revision 14340 - 2015-06-19 22:09 - Jean-Philippe Lang

Fixed r14339 for when closing the dialog by using the upper-right cross (#19851).

Revision 14341 - 2015-06-19 22:12 - Jean-Philippe Lang

Fixed wrong password rendering broken by r14339 (#19851).

Revision 14342 - 2015-06-19 22:14 - Jean-Philippe Lang

Adds french translation (#19851).

Revision 14343 - 2015-06-19 22:20 - Jean-Philippe Lang

Removed extra blank lines (#19851).

Revision 14344 - 2015-06-19 22:25 - Jean-Philippe Lang

Tests that submitted data is present in the sudo form (#19851).

Revision 14345 - 2015-06-19 22:42 - Jean-Philippe Lang

Adds a UI test (#19851).

Revision 14346 - 2015-06-19 22:45 - Jean-Philippe Lang

Removed extra blank lines (#19851).

Revision 14352 - 2015-06-19 23:00 - Jean-Philippe Lang

Adds translation strings (#19851).

Revision 14353 - 2015-06-19 23:17 - Jean-Philippe Lang

Make the sudo timeout configurable (#19851).

Revision 14354 - 2015-06-20 00:23 - Jean-Philippe Lang

Set a default timeout value (#19851).

Revision 14359 - 2015-06-20 12:57 - Jean-Philippe Lang

Fixed test error (#19851).

History

#1 - 2015-05-19 13:35 - Jan Niggemann (redmine.org team member)

I like the idea, thank you for providing a patch!

#2 - 2015-06-14 06:24 - Toshi MARUYAMA

- Target version set to 3.1.0

#3 - 2015-06-16 21:23 - Jean-Philippe Lang

This would be a nice addition for 3.1.0 indeed but this feature may not be wanted for all Redmine instances. I think we should let people decide whether or not this feature is enabled. The configuration file would be a good place to have this setting (obviously it should not be possible to turn it on/off from the web interface).

#4 - 2015-06-19 22:44 - Jean-Philippe Lang

- Tracker changed from Patch to Feature

- Subject changed from [Feature] Require password re-entry for sensitive actions (sudo mode) to Sudo mode: Require password re-entry for sensitive actions (optional)

- Status changed from New to Closed

- Assignee set to Jean-Philippe Lang

- Resolution set to Fixed

The patch and a few changes are committed.

Files